

an application programming interface which provides interface between said secure container and a third party software;

said secure container processes the requests coming from said third party software through said application programming interface;

said secure container validates signatures of one or more documents to verify that said one or more documents are compatible with said secure container;

in the case of verification of compatibility of said one or more documents with said secure container, said secure container initiates loading one or more dynamically linked libraries; and

in the case of incompatibility of said one or more documents with said secure container, said secure container refuses to load any data coming through said application programming interface.

16. A digital right management system according to claim 15, wherein said third party software comprises a rendering engine.

17. A digital right management system according to claim 16, wherein said rendering engine is connected to a printer.

18. A digital right management system according to claim 16, wherein said rendering engine is connected to a computer monitor.

19. A digital right management system according to claim 16, wherein said rendering engine is connected to a handheld device.

20. A digital right management system according to claim 16, wherein said rendering engine is connected to a wireless device.

21. A digital right management system according to claim 16, wherein said rendering engine is connected to a device with one or more optical communication ports.

22. A digital right management system according to claim 15, wherein said secure container performs rights management.

23. A digital right management system according to claim 15, further comprising one or more self-protecting documents.

24. A digital right management system according to claim 15, further comprising one or more structured storages.

25. A digital right management system according to claim 15, further comprising one or more structured file systems.

*Q2* 26. A digital right management system according to claim 15, further comprising information specifying content types.

27. A digital right management system according to claim 15, further comprising information specifying licenses.

28. A digital right management system according to claim 23, wherein said secure container detects whether any of said one or more self-protecting documents is tampered with.

29. A digital right management system according to claim 15, further comprising an encryption engine.

30. A digital right management system according to claim 15, further comprising a user-interface module.

31. A digital right management system according to claim 30, wherein said user-interface module includes one or more menus or toolbars.

32. A digital right management system according to claim 15, wherein said secure container acts as a shell to be compatible to the third-party plug-ins which are designed based on a predetermined specification of said secure container's interface.

33. A digital right management system according to claim 15, further comprising a software development kit that enables the creation of applications to protect, distribute, and consume content.

34. A digital right management system according to claim 15, wherein said system is connected to one or more storefronts.

35. A digital right management system according to claim 15, wherein said system is connected to one or more backoffices.

36. A digital right management system according to claim 15, wherein said system creates one or more rights labels.

37. A digital right management system according to claim 15, wherein said system creates one or more rights templates.

38. A digital right management system according to claim 15, wherein said system creates one or more metadata.--